Vacancy

CLP Holdings Limited
Group Operations
Group Security
Incident Response Specialist
[Ref.: CLPH-GO-GS-IRS]

We are looking for a high caliber individual to join our Group Security Team as Incident Response Specialist. The appointee will deliver the Company's cyber incident detection and response capability. Key responsibilities include:

The Position Profile:

- To quickly and efficiently detect rogue activity i.e. events that indicate an active attack on CLPs networks. Work with internal teams to voice out identified monitoring blind spots in the existing enterprise and work as required to ensure that these gaps are closed, and also to launch suitable improvement programs where necessary. In addition to addressing weaknesses in existing infrastructure, the future planned architecture for monitoring and detection must address changes to the Cyber Threat.

- Working with the Cyber Intelligence Team to maintain SME in the Tools, Techniques and Procedures (TTPs) of threat actors.

- Work with the outsourced provider (Symantec) to delivers monitoring of CLP networks across all the regions effectively. To be part of a highly specialized team enhancing CLP's internal monitoring and response capability.

- Be a genuine subject matter expert and add real value when events are escalated for arbitration.

- Work with key stakeholders (e.g. Site-based IT staff) to close-out security events i.e. to ascertain the root cause of the event and whether it is worthy of investigation, escalation or immediately declaring as a security incident (e.g. an attack).

- Take up the accountability on operational incident response by taking place on the Cyber Security on-call roster and be available on a 24hr emergency basis. Once an attack has been detected and validated, the incumbent must ensure that appropriate timely response is instigated to remediate (or contain) the attack. Moreover, to take those appropriate immediate response calls on their own authority. Thereafter, make appropriate and timely escalation and that key stakeholders are actively engaged, and also to ensure all actions are recorded in the Incident/Case management system.

- Implement a complete technical vulnerability management cycle for all CLP Group assets and networks, including vulnerability scanning, risk rating, remediation tracking, management reporting, feeding the vulnerability intelligence into incident management.

- Partner and align with IT operations, business operations and external parties (for example, external security service providers, law enforcements, etc) to form a smooth incident management, coordinating efforts as required to ensure that overall incident management mission is achieved.

- With a solid understanding of forensic and incident response casework, to provide ownership with maintaining case information, chain of custody reporting, and full documentation of issues from identification through remediation.

Requirements:

- University Degree in Computer Science, Information Technology or equivalent.

- A minimum of 5 years' IT experience with Microsoft enterprise technologies including but not limited to Windows, Active Directory, TMG, IIS etc; Open source technologies such as Linux; virtualization technologies such as VMware and Hyper-V; and hands-on experience in TCP/IP networking, firewalls, VPN, intrusion prevention systems, network security monitoring, network vulnerability scanning.

- Familiar with best-in-class IT & ICS security technologies by leading suppliers such as Cisco, Checkpoint, Palo Atos, Symantec, FireEye and Juniper.

- Proven knowledge of security incident response on both IT and OT environments; and prior experience in security operations center coordination/management is a must.

- Strong cyber incident investigation skills, and malware investigation.

- Strong written and verbal communication skills, including the ability to gather and critically evaluate information and prepare written documents that clearly and concisely identify the issues presented and their proposed resolution.

- Strong reasoning competence to investigate, analyze and draw appropriate conclusions.

- Excellent organizational, collaboration and interpersonal skills.

- Fluent in spoken and written English, and capability in both spoken and written Chinese (Putonghua and simplified Chinese) are advantageous.

Please apply by sending email to ghr@clp.com.hk giving a detailed C.V., including academic qualification, career history, current and expected salary, major achievements and personal attributes on or before **30 June 2021.**

Important: To facilitate our easy tracking please use a unique file name for all attachments and your email subject box in this format: CLPH-GO-GS-IRS_Last Name_First Name_Other Names (if applicable)

Applicants not invited for interview within 6 weeks from the closing date may assume their applications unsuccessful.

Information provided will be for recruitment purpose within the CLP Group and only short-listed candidates will be contacted. We comply with all applicable laws and regulations of HKSAR in handling applications. For details of the Personal Information Collection Statement, please visit our website: http://clp.to/engPICS

For further information on our company, please visit our website: https://www.clpgroup.com/

Date Exhibited: 03.06.2021
Date Withdrawn: 30.06.2021

Information Classification: PROPRIETARY

(本項職位空缺只備英文版本)